BRIEF DESCRIPTION OF THE DRAWINGS

FIGURE 1 is a schematic the preferred embodiment of the network system of the present invention;

FIGURE 1A is a schematic the first preferred embodiment of the backside of a computing device of the present invention for use with the data security system of FIGURE 1, the computing device (30C) enabling biometric authentication prior to accessing network data, the computing device (30C) being handheld and portable, the handheld computer (30C) being pen-based, the handheld computer (30C) comprising a stylus (50) for operating such computing device (30C), the computer (30C) being remote from a host processor (12) and enabling access to network data, the computer (30C) including a pair of fingerprint sensors (15) embedded in the casing of the handheld computer (30C), one fingerprint sensor (15) capturing a print image of the user's thumb and the second fingerprint image sensor (15) capturing a print image of the user's index finger, both being of the user's left hand;

FIGURE 1B discloses the stylus of FIGURE 1A, the stylus including a fingerprint sensor in the stylus barrel for enabling capture of a fingerprint image when the stylus is grasped;

FIGURE 1C discloses the front-side of the handheld computer of FIGURE 1A, the handheld computer including a fingerprint sensor embedded into the casing of the handheld computer at a site such that the image of the thumb of the user is captured during usage of the handheld computer;

FIGURES 2A and 2B disclose a second preferred embodiment of the front-side and the backside respectively of the computing device of the present invention for use either with the data security system of FIGURE 1 or as a stand alone unit with secure data therewithin, the computing device being handheld and portable, not necessarily pen-based and if pen-based with no fingerprint sensor in the stylus, the computing device being remote from a host processor and enabling access to network data, the computing device including a pair of fingerprint sensors embedded in the casing, one fingerprint sensor capturing a print image of the user's thumb and the second fingerprint image capturing a print image of the user's index finger, both being of the user's left hand;

FIGURE 3A discloses another preferred embodiment of a computing device for use with the

accessing data and data entry to the data security system of the FIGURE 1;

FIGURES 9A and 9C disclose a simplified logic diagram of one preferred embodiment for requesting access to high security data of the data security system of FIGURE 1, the high security data access request requiring a match authentication of a pair of user fingerprints;

FIGURES 9B and 9C disclose a simplified logic diagram of another preferred embodiment for requesting access to high security data for the data security system of FIGURE 1, the system supplying the user with misinformation if the remote computer is counterfeit;

FIGURE 10A discloses a simplified layout for a user record of one preferred embodiment of the data security system of FIGURE 1;

FIGURE 10B discloses a simplified layout for a data access record for the preferred embodiment of the data security system of FIGURE 10A;

FIGURE 10C discloses a simplified layout for a remote computer record for the preferred embodiment of the data security system of FIGURE 10A;

FIGURE 11 discloses a simplified flowchart for performing a network security audit of the data security system of FIGURE 1;

FIGURE 12A discloses a simplified curve analysis for a regular security environment with the data security system of FIGURE 1, where the threshold position is located at the juncture of the normal curve for authorized users and the normal curve for unauthorized users; and

FIGURE 12B discloses a simplified curve analysis showing for high-security applications with the data security system of FIGURE 1, the curve analysis being similar to FIGURE 12A, where the position of the threshold has been repositioned to minimize false negatives.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to the drawings, FIGURE 1 discloses the preferred embodiment of the data security system of the present invention. The data security system comprises a host processor (12) and a plurality of computing devices (30A, 30B, 30C, 30D). The host computer (12) includes confidential data

that is to be accessed only by authorized users. Some of the computing devices (30C and 30D) are wireless and remote from the host computer (12). The wireless computing devices (30C and 30D) are portable and handheld - and may be pen-based (30C) as shown in FIGURES 1A, 1B, and 1C, or not pen-based (30D) as shown in FIGURES 2A and 2B.

The computing device includes a sensor for capture of a user biometric image - preferably a fingerprint sensor (15). The fingerprint sensor (15) captures an image of a user's finger prior to each request to access data - guarding against unauthorized access to network data (a network security breach). The fingerprint image [~~sensor~~] can also be captured prior to each request to enter new data to prevent contamination of network data.

The capture of the user biometric image is available at continual intervals during routine computer usage. Preferably, the image is captured and compared against a system reference image prior to each request for data access. In another embodiment, the capture occurs continually during predetermined intervals independent of any data access or entry requests. The continual monitoring of user identity provides an added layer of system security.

The capture of the user biometric image is incidental to routine computer usage. The biometric authentication is seamless, as the computer user need only hold the handheld computer is his/her hand similar to holding a conventional handheld computer. The capture of the biometric image is incidental manner to computer operation.

As shown in FIGURE 2A and 2B, at least one fingerprint sensor (15) is positioned at one or more strategic sites such that a portion of the hand of the user is in continuous contact therewith during usage of the processor (30D), enabling a continual authentication of the identity of the user with each request for access to each secure record. The fingerprint authentication is captured in an incidental manner as the data request is submitted from the handheld computer (30D) to the host processor (12) enabling user identity authentication simultaneously with each request to access the secure record. As shown, the processor (30D) includes sensors (15) to capture a thumbprint, the print of the index finger, and a palm print. Also, a palm print sensor (17) can be disposed on the back surface of the computing device (30D) of the present invention to supplement or complement the fingerprint sensors (15). Multiple sensors are recommended for high-security applications (see for example FIGURES 9A and 9B).

FIGURE 3A discloses the frontside of another embodiment of a processor device (20a) for use in another preferred embodiment of the data security system of the present invention. The fingerprint sensor (15) is positioned in the casing (22) of a palm computer (20a), the casing (22) being used to house the palm computer (20a) when used and stored. The casing (22) may also be a wallet or pouch in digital engagement with the processor (20a), either through wire or a wireless mode - enabling identity authentication whenever network access to data is required. The principle advantage of this approach is that registration is conducted through the casing (22) and the computers need not be altered (off the shelf). FIGURE 3B discloses yet another full-screen processor (20b) for use in the data security system of the present invention. These processors (20b) are sometimes referred to as handheld computers in the literature, but are referred to as full-screen processors herein for clarity. The screen is roughly the size of a screen of a PC, except that the computer does not have a conventional keypad. A fingerprint sensor (15) is disposed on one side of the full-screen computer.

FIGURE 4A discloses another preferred embodiment of a computing device (30E) for use in the data security system of the present invention. The handheld computing device (30E) includes a facial image biometric sensor (16) that captures a facial biometric when data access is made from the handheld computing device (30E). FIGURE 4B discloses yet another preferred embodiment of a computing device (30F) for use in the data security system of the present invention. The computing device (30F) is a handheld computer, having a palm image sensor (17) disposed on the backside thereof.

The strategic positioning of individual and multiple sensors depends on the size and shape of the individual computer, and the size of the hands of the computer user. And, it is advised that either the location of the sensors is symmetrical (both sides of the processor) to accommodate both left-handed and right-handed users. Alternatively, some processors can be designed for right-handed users and others for left-handed users.

Referring now to FIGURE 5, the user registers his or her prints by submitting the thumb, index finger, and/or palm prints to the network in a secure process. The reference print is preferably stored in the host processor for security purposes to prevent user access and tampering. The prints may need to be stored in the system also. Subsequently, when network access is requested, the relevant print or prints are captured and compared against